Exhibit K

LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

FBI, Secret Service Warn Of Targeted Ransomware

By **Ben Kochman**

Law360, New York (November 18, 2019, 9:44 PM EST) -- Senior FBI and U.S. Secret Service officials said Monday that cybercriminals are increasingly using ransomware to target vulnerable entities like hospitals and municipalities, and urged victims to report attacks to authorities regardless of whether they capitulate and pay ransoms.

"We don't necessarily have the data that shows that the incidents of ransomware are rising, but what we do see is that those incidents are more targeted against victims that have the highest incentive to pay," said Tonya Ugoretz, deputy assistant director at the FBI's Cyber Division, during a panel at NYU's Center for Cybersecurity.

The ransom amounts being requested on average are rising, Ugoretz added Monday. Ransomware victims **often cave** to their attackers' demands, industry attorneys have told Law360, despite the FBI's official guidance that doing so could embolden cybercriminals to launch more attacks and incentivize others to try their hand at cybercrime.

Victims have included the city of Atlanta, which has said that it ended up spending more than $10 million to **recover from** a cyberattack. Riviera Beach and Lake City in Florida have said that they paid $600,000 and $500,000 in bitcoin, respectively, this summer after failing to recover their data on their own.

Entities like smaller municipalities and hospitals are attractive to ransomware criminals, cybersecurity experts say, because they often have lesser IT defenses and a high incentive to regain access to their data quickly.

The bureau softened its stance on ransomware payments somewhat last month, writing in updated guidance that the FBI "understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers."

Michael D'Ambrosio, assistant director of the office of investigations at the Secret Service, which also investigates ransomware attacks, acknowledged on Monday that a blanket ban on entities paying ransoms is unrealistic.

"Law enforcement right now is not going to come out and say you cannot pay ransomware," he said during the panel. "However, it seems to be that you would want to do it in conjunction with law enforcement in order to try to find the individuals that have perpetrated the crime."

"There may be some information in there that we may be able to help you with," D'Ambrosio added, saying that in some cases the government has been able to help victims track down decryption keys and reclaim their data.

Ugoretz also urged ransomware victims to cooperate with federal authorities, who say they have been successful in tracking down ransomware attackers, even if it can be difficult to extradite the attackers to U.S. courts. For example, a federal investigation led to the **December indictment** of two Iranian men for the Atlanta attack, which court papers say was part of an international scheme in which the duo extorted dozens of hospitals, cities and public institutions.

Companies who invite the FBI into their systems to investigate suspected ransomware will be treated as victims, Ugoretz said, in an attempt to assuage fears that the bureau's agents, once granted access, could start looking around for potential evidence of corporate wrongdoing.

"We're not there on a fishing expedition," Ugoretz said. "We're not there to run in with green jackets and make a very noisy response ... We have a long history of treating victims like victims."

Ugoretz also defended the Justice Department's recent trend of so-called "name-and-shame" indictments, which target **alleged cybercriminals** based in countries like China, Russia and Iran, with whom the U.S. does not have extradition agreements.

U.S. authorities do sometimes find a way to extradite such defendants, Ugoretz said, pointing to recent cases including last week's appearance of 29-year-old Russian national Aleksei Burkov in Virginia federal court, where he is charged with operating a payment card fraud ring. Such indictments are key in sending a message to the rest of the world about what types of cybercrime the U.S. finds unacceptable, Ugoretz added.

"We talk a lot about norms in cyberspace," she said during the panel, "and these indictments are one way of signaling what is counternormative behavior."

--Editing by Daniel King.
